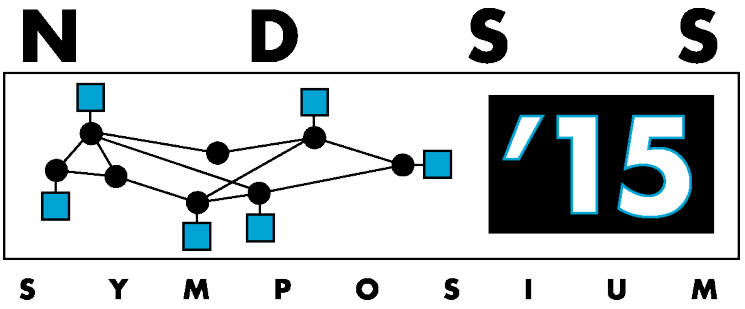
Proceedings

2015

Network and Distributed System Security Symposium



Proceedings

2015

Network and Distributed System Security Symposium

February 8 – 11, 2015
San Diego, California

Sponsored by the
Internet Society

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108

Address your correspondence to: Senior Events Manager, Internet Society, 1775 Wiehle Avenue, Suite 201, Reston, Virginia 20190-5108, U.S.A., tel. +1 703 439 2120, fax +1 703 326 9881, ndss@isoc.org.

The papers included here comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.

ISBN Number (Digital Format) 1-891562-38-X

Additional copies may be ordered from:

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108
tel +1 703.439.2120
fax +1 703.326.9881
http://www.internetsociety.org

Table of Contents

CopperDroid: Automatic Reconstruction of Android Malware Behaviors
K. Tam, S.J. Khan, A. Fattori, L. Cavallaro

DeepDroid: Dynamically Enforcing Enterprise Policy on Android Devices
X. Wang, K. Sun, Y. Wang, J. Jing

SESSION 3: Detection, Analysis, Prevention & Response – Part I
Session Chair: Stelios Sidiroglou-Douskos, Massachusetts Institute of Technology

VTint: Protecting Virtual Function Tables' Integrity
C. Zhang, C. Song, K. Zhijie Chen, Z. Chen, D. Song

Phoneypot: Data-driven Understanding of Telephony Threats
P. Gupta, B. Srinivasan, V. Balasubramaniyan, M. Ahamad

SeCReT: Secure Channel between Rich Execution Environment and Trusted Execution Environment
J. Jang, S. Kong, M. Kim, D. Kim, B. B. Kang

FreeSentry: Protecting Against Use-After-Free Vulnerabilities Due to Dangling Pointers
Y. Younan

EKHunter: A Counter-Offensive Toolkit for Exploit Kit Infiltration
B. Eshete, A. Alhuzali, M. Monshizadeh, P. Porras, V.N. Venkatakrishnan, V. Yegneswaran

SESSION 4: Privacy – Part I
Session Chair: Srdjan Capkun, ETH Zürich

Machine Learning Classification over Encrypted Data
R. Bost, R. Ada Popa, S. Tu, S. Goldwasser

Gracewipe: Secure and Verifiable Deletion under Coercion
L. Zhao, M. Mannan

Privacy Preserving Payments in Credit Networks: Enabling trust with privacy in online marketplaces
P. Moreno-Sanchez, A. Kate, M. Maffei, K. Pecina

Checking More and Alerting Less: Detecting Privacy Leakages via Enhanced Data-flow Analysis and Peer Voting
K. Lu, Z. Li, V.P. Kemerlis, Z. Wu, L. Lu, C. Zheng, Z. Qian, W. Lee, G. Jiang

DEFY: A Deniable, Encrypted File System for Log-Structured Storage
T.M. Peters, M.A. Gondree, Z.N.J. Peterson

SESSION 5: Detection, Analysis, Prevention & Response – Part II
Session Chair: Heng Yin, Syracuse University

Preventing Use-after-free with Dangling Pointers Nullification
B. Lee, C.Y. Song, Y. Jang, T. Wang, T. Kim, L. Lu , W. Lee

StackArmor: Comprehensive Protection from Stack-based Memory Error Vulnerabilities for Binaries
X. Chen, A. Slowinska, D. Andriesse, H. Bos, C. Giuffrida

Isomeron: Code Randomization Resilient to (Just-In-Time) Return-Oriented Programming
L. Davi, C. Liebchen, A-R. Sadeghi, K.Z. Snow, F. Monrose

Thwarting Cache Side-Channel Attacks Through Dynamic Software Diversity
S. Crane, R. Homescu, S. Brunthaler, P. Larsen, M. Franz

SESSION 6a: Detection, Analysis, Prevention & Response – Part III

Principled Sampling for Anomaly Detection
B. Juba, C. Musco, F. Long, S. Sidiroglou-Douskos, M. Rinard

Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes
M. El Massad, S. Garg, M. Tripunitara

Opaque Control-Flow Integrity
V. Mohan, P. Larsen, S. Brunthaler, K.W. Hamlen, M. Franz

SESSION 6b: Privacy – Part II

Bloom Cookies: Web Search Personalization without User Tracking
N. Mor, O. Riva, S. Nath, J. Kubiatowicz

NSEC5: Provably Preventing DNSSEC Zone Enumeration
S. Goldberg, M. Naor, D. Papadopoulos, L. Reyzin, S. Vasant, A. Ziv

SESSION 7: Social Networks and Cloud Services
Session Chair: Dongyan Xu, Purdue University

Predicting Users' Motivations behind Location Check-Ins and Utility Implications of Privacy Protection Mechanisms
I. Bilogrevic, K. Huguenin, S. Mihaila, R. Shokri, J-P. Hubaux

On Your Social Network De-anonymizablity: Quantification and Large Scale Evaluation with Seed Knowledge
S. Ji, W. Li, N.Z. Gong, P. Mittal, R. Beyah

Efficient RAM and Control Flow in Verifiable Outsourced Computation
R.S. Wahby, S. Setty, Z. Ren, A.J. Blumberg, M. Walfish

Integro: Leveraging Victim Prediction for Robust Fake Account Detection in OSNs
Y. Boshmaf, D. Logothetis, G. Siganos, J. Leria, J. Lorenzo, M. Ripeanu, K. Beznosov

SESSION 8: Authentication
Session Chair: Zhenkai Liang, National University of Singapore

Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords
J. Blocki, S. Komanduri, L. Cranor, A. Datta

ABY - A Framework for Efficient Mixed-Protocol Secure Two-Party Computation
D. Demmler, T. Schneider, M. Zohner

Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics
S. Eberz, K.B. Rasmussen, V. Lenders, I. Martinovic

Knock Yourself Out: Secure Authentication with Short Re-Usable Passwords
B. Guldenring, V. Roth, L. Ries

Verified Contributive Channel Bindings for Compound Authentication
K. Bhargavan, A. Delignat-Lavaud, A. Pironti

SESSION 9: Web Security – Part II
Session Chair: Ben Livshits, Microsoft Research

The Devil is in the Constants: Bypassing Defenses in Browser JIT Engines
M. Athanasakis, E. Athanasopoulos, M. Polychronakis, G. Portokalidis, S. Ioannidis

Exploiting and Protecting Dynamic Code Generation
C. Song, C. Zhang, T. Wang, W. Lee, D. Melski

Too LeJIT to Quit: Extending JIT Spraying to ARM
W. Lian, H. Shacham, S. Savage

Run-time Monitoring and Formal Analysis of Information Flows in Chromium
L. Bauer, S. Cai, L. Jia, T. Passaro, M. Stroucken, Y. Tian

SESSION 10: Network Security
Session Chair: Ivan Martinovic, University of Oxford

Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks
P-A. Vervier, O. Thonnard, M. Dacier

SPHINX: Detecting Security Attacks in Software-Defined Networks
M. Dhawan, R. Poddar, K. Mahajan, V. Mann

Securing the Software Defined Network Control Layer
P. Porras, S. Cheung, M. Fong, K. Skinner, V. Yegneswaran

Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures
S. Hong, L. Xu, H. Wang, G. Gu

SESSION 11: Detection, Analysis, Prevention & Response – Part IV
Session Chair: Christopher Kruegel, University of California Santa Barbara

Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware
Y. Shoshitaishvili, R. Wang, C. Hauser, C. Kruegel, G. Vigna

vfGuard: Strict Protection for Virtual Function Calls in COTS C++ Binaries
A. Prakash, X. Hu, H. Yin

P2C: Understanding Output Data Files via On-the-Fly Transformation from Producer to Consumer Executions
Y. Kwon, F. Peng, D. Kim, K. Kim, X. Zhang, D. Xu, V. Yegneswaran, J. Qian

No More Gotos: Decompilation Using Pattern-Independent Control-Flow Structuring and Semantics-Preserving Transformations
K. Yakdan, S. Eschweiler, E. Gerhards-Padilla, M. Smith

General Chair's Message

It is my pleasure to welcome you to the 22nd Internet Society Symposium on Network and Distributed System Security (NDSS15).

From our very first workshop and continuing today, NDSS has striven to maintain the superior quality of our technical program. Our research domain continues to emphasize practical applications of security based on solid theoretical foundations. The program stretches from canonical to current, and includes both the theoretical and the pressing needs. This scope, along with a willingness to consider potentially controversial or unusual research, is the essential beauty of NDSS.

Again for our second year we have optional SENT and USEC full-day Workshops (Security of Emerging Network Technologies and Usable Security) on Sunday. These will bring together academic and industry researchers to discuss security problems, challenges, and potential solutions of emerging networking technologies such as Software Defined Networks, Named-Data-Networking and Cellular networks.

The main program this year packs a lot into three full days and includes 11 sessions. They cover a variety of current topics including a 4-part multiple session on Detection, Analysis, Prevention and Response. Other sessions cover such areas as Social and Cloud Services, Privacy, Web Security and Mobile Security. Our keynote speaker this year is Dr. Stephen Farrell, a research fellow in the department of Computer Science at Trinity College Dublin.

Although the symposium revolves around the technical presentations, there is far more to the experience. Take advantage of the hall track, the reception, the lunches, and the Tuesday banquet to meet new colleagues. These discussions are invaluable parts of the process of disseminating and discussing information. And finally, remember to save some time to enjoy our fantastic city.

This symposium is possible only through the hard work of many people. I would like to thank following: the NDSS steering group for charting a course for the conference that keeps its focus current, relevant, and practical; the conference committee for dealing with all the details to put together such an event and to publish its proceedings; and the Internet Society and its staff for their fantastic job with registration and all the work leading up to the conference. This meeting is as enjoyable and as successful as it is because of the efforts of these people -- it is no exaggeration to say that NDSS simply would not happen without each of their contributions.

The quality of this conference directly depends upon the quality of the papers accepted. The program committee, under the direction of Program Chair Engin Kirda of Northeastern University, has done a fantastic job and has selected an extraordinary set of papers. I thank Engin and the entire program committee for their expertise, hard work, and dedication. I also want to thank Adrian Perrig and Gene Tsudik for organizing and chairing the SENT workshop and Jens Grossklags for the organizing and chairing of the USEC workshop. Lastly, I also thank the authors who submitted papers and the speakers who are present; YOU are the core of this symposium.

I am also grateful for our sponsors, as it would be impossible to hold such an event without them. Our sponsors are the Internet Society for overall sponsorship, Cisco Systems for Gold Sponsorship; Afilias, Qualcomm, and the San Diego Supercomputer Center @ UCSD (SDSC) for Silver sponsorship; Research at Google, IBM Research, and Microsoft Research for Bronze sponsorships, and IEEE Security and Privacy Magazine as our media sponsor. The conference is organized by the Internet Society, in cooperation with USENIX.

I would also like to thank my organization, the San Diego Supercomputer Center at the University of California San Diego, for supporting my involvement with this symposium over the last 22 years.

Finally, I want all of you to know that I view it as a great honor to chair this conference, one where the attendees and speakers are some of the finest minds in computer network security.

Thomas Hutton
General Chair, NDSS'15
San Diego Supercomputer Center
University of California, San Diego

Program Chair's Message

It is my great pleasure to welcome you to the 22nd Annual Network & Distributed System Security Symposium (NDSS 2015), held at the Catamaran Resort Hotel and Spa in San Diego, CA, United States on February 8-11, 2015. I was very honored to chair this year's NDSS -- a conference that fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of network and distributed systems security technologies.

This year, NDSS received 300 valid submissions (i.e., not counting papers that clearly violated the submission guidelines). Submissions were evaluated on the basis of their technical quality, novelty, and significance. Papers went through two rounds of review. Reviewing culminated in a one-and-a-half-day in-person program committee meeting at Northeastern University in Boston, at which 50 papers (approximately 17%) were selected to appear at NDSS.

Organizing a conference as large as NDSS is a substantial endeavor, and I'd like to extend my sincere thanks to everyone who contributed his or her time and effort. I'd also like to specifically thank a few individuals who made particular contributions to NDSS 2015. Nicole Armstrong and Terry Weigler handled most of the logistics of organizing the conference, as well as the task difficult task of guiding a new program chair who was not familiar with the organizational specifics of NDSS. Srdjan Capkun served as the shadow chair and made my life as chair a lot easier with his advice, suggestions, and oversight. Also, it was great fun to work Srdjan. Thanks chiefly to the efforts and persistence of David Balenson, the Publications Chair, NDSS 2015 proceedings and papers have been assigned digital object identifiers (DOIs), enabling easier search and indexing. I would also like to thank everyone who accepted my invitation to serve on the program committee. I was very impressed because almost everyone was physically present at the PC meeting in Boston. It was my pleasure and honor to have worked with you to put together the program for NDSS 2015. Also crucial to the success of NDSS are the authors who submitted papers---thank you!---and the attendees. Welcome to NDSS, and I hope you find the program informative and stimulating.

Engin Kirda
Program Chair, NDSS'15
Northeastern University

Program Committee

Engin Kirda (Chair), Northeastern University

Ahmad-Reza Sadeghi, TU Darmstadt

Alina Oprea, RSA Laboratories

Apu Kapadia, Indiana University Bloomington

Ari Juels, Cornell Tech

Ben Livshits, Microsoft Research Redmond

Christian Kreibich, Lastline Inc / International Computer Science Institute, Berkeley

Christopher Kruegel, University of California, Santa Barbara

David Brumley, Carnegie Mellon University

David Wagner, University of California, Berkeley

Davide Balzarotti, EURECOM, France

Dongyan Xu, Purdue University

Georgios Portokalidis, Stevens Institute of Technology

Gianluca Stringhini, University College London, UK

Guofei Gu, Texas A&M University

Hayawardh Vijayakumar, Samsung

Heng Yin, Syracuse University

Ivan Martinovic, Oxford University, UK

Juan Caballero, IMDEA, Spain

Long Lu, Stony Brook University

Manuel Egele, Boston University

Michael Bailey, University of Illinois at Urbana-Champaign

Nicolas Christin, Carnegie Mellon University

Patrick Traynor, University of Florida

Prateek Mittal, Princeton University

Roberto Perdisci, University of Georgia

Robin Sommer, International Computer Science Institute, Berkeley

Somesh Jha, University of Wisconsin Madison

Srdjan Capkun, ETH Zurich, Switzerland

Stelios Sidiroglou-Douskos, Massachusetts Institute of Technology

Stephen McCamant, University of Minnesota

Tim Leek, MIT Lincoln Labs

Ting-Fang Yen, E8 Security

Venkat Venkatakrishnan, University of Illinois, Chicago

Wenke Lee, Georgia Institute of Technology

William Robertson, Northeastern University

William Enck, North Carolina State University

XiaoFeng Wang, Indiana University Bloomington

Yongdae Kim, KAIST, South Korea

Zhenkai Liang, National University of Singapore, Singapore

Zhichun Li, NEC Labs America

Zhiqiang Lin, University of Texas, Dallas

Organizing Committee

General Chair and Local Arrangements Chair

Thomas Hutton
San Diego Supercomputer Center
University of California, San Diego
hutton@ucsd.edu

Program Chair

Engin Kirda
Northeastern University
ek@ccs.neu.edu

Publications Chair and Historian

David Balenson
SRI International
david.balenson@sri.com

Workshop Chair

Matthew Smith
Rheinische Friedrich-Wilhelms-Universität Bonn
smith@cs.uni-bonn.de

Conference Coordinator

Terry Weigler
Internet Society
weigler@isoc.org

Event Manager, Publicity Chair, and Sponsorship Coordinator

Nicole Armstrong
Internet Society
armstrong@isoc.org

Steering Group

Co-Chairs

Thomas Hutton
San Diego Super Computer Center
University of California, San Diego

Karen O'Donoghue
Internet Society

Administrative Coordinator

Terry Weigler
Internet Society

Steering Group Members

Michael Bailey
University of Illinois at Urbana-Champaign

David Balenson
SRI International

Davide Balzarotti
EURECOM

Lujo Bauer
Carnegie Mellon University

Srdjan Capkun
ETH Zurich, Switzerland

Deb Frincke
National Security Agency

Yongdae Kim
Korea Advanced Institute of Science and Technology

David Molnar
Microsoft Research

Clifford Neuman
University of Southern California

Deborah Shands
Aerospace Corporation

Paul Syverson
Naval Research Lab

Doug Szajda
University of Richmond

Helen Wang
Microsoft Research